CLAIMS

1. A security apparatus for a wireless LAN, comprising:

a plurality of end stations; and

a Public Access Point (PAP) for providing a plurality of virtual Basic Service Sets (BSS) from within a single physical access point (AP);

wherein any number of said end stations can belong to a virtual BSS;

wherein said PAP appears to said end stations as multiple physical access points, one AP for each virtual BSS.

2. The apparatus of Claim 1, said PAP provisioning a plurality of separate LAN segments while providing separate link privacy and integrity for each of said LAN segments.

3. The apparatus of Claim 1, wherein all of said end stations, and any local file servers and other devices associated with said LAN, are associated with a virtual access point; and wherein all virtual access points arise from a same physical PAP.

4. The apparatus of Claim 1, further comprising:

a plurality of PAPs; and

a location-update protocol for updating forwarding tables of bridges that connect said PAPs together.

5. The apparatus of Claim 1, further comprising:

a finebridging method for limiting communications between all said end stations that belong to a virtual BSS.

6. A security apparatus for a wireless LAN, comprising:

a plurality of 802.11 end stations;

a Public Access Point (PAP), said PAP comprising a personal virtual bridged LAN (PVLAN) instantiated into a virtual 802.11 Basic Service Set (BSS) from within a single physical access point (AP).

7. A secure wireless network, comprising:

a virtual 802.11 Basic Service Set (BSS);

a plurality of stations, each of said stations having a hardware (MAC) address;

all said stations in said virtual BSS sharinga group security association; and

one of said stations in said virtual BSS comprising a public access point (PAP).

8. The network of Claim 7, said group security association of each station comprising:

an encryption key and an authentication code key.

9. The network of Claim 7, wherein exactly one of said stations in said virtual BSS is a public access point for bridging an 802.11 Wireless Medium (WM) and an 802.11 Distribution System Medium (DSM).

10. The network of Claim 7, said group security association further comprising:

a unique unicast security association for every station in said virtual BSS;

wherein said security association is shared between each station and said PAP of said virtual BSS.

11. The network of Claim 7, further comprising:

a plurality of virtual BSSs, wherein each virtual BSS has its own identifier, (BSSID).

12. The network of Claim 11, said BSSID comprising:

a virtual MAC address for said virtual BSS.

13. The network of Claim 12, wherein said PAP receives a frame from an 802.11 Wireless Medium (WM) destined for one of its virtual MAC addresses; and wherein said PAP transmits a frame to said WM using one of its virtual MAC addresses as a source MAC address of said frame.

14. The network of Claim 7, further comprising:

a plurality of virtual BSSs supported by a shared TSF (Timing Synchronization Function), DCF (Distributed Coordination Function), and, optionally, a PCF (Point Coordination Function), at a single PAP.

15. The network of Claim 7, each PAP further comprising:

a single NAV (Network Allocation Vector) and PC (Point Coordinator).

16. The network of Claim 7, wherein a PAP can belong to more than one virtual BSS.

17. The network of Claim 7, wherein any station that is not a PAP can belong to at most one virtual BSS.

18. The network of Claim 7, further comprising:

a virtual bridged LAN (VLAN) for bridging a virtual BSS with another virtual BSS by connection of each virtual BSS's PAP.

19. The network of Claim 18, wherein the PAP of each virtual BSS connects to a Distribution System (DS) via a trunked or untagged port of a VLAN-aware bridge.

20. The network of Claim 19, wherein frames transmitted to said DS carry VLAN tags known to a Distribution System Medium (DSM).

21. The network of Claim 20, wherein said PAP maintains a DSM VLAN mapping that maps a VLAN tag to a virtual BSS identifier (BSSID).

22. The network of Claim 7, said virtual BSS comprising any of:

a Class-1 and a Class-3 virtual BSS;

wherein a PAP supports exactly one Class-1 virtual BSS and one or more multiple Class-3 virtual BSSs;

wherein a Class-1 virtual BSS is the only virtual BSS which a station is allowed to occupy while it is in 802.11 State 1 or 2, as governed by said PAP;

wherein when in State 3, a station is allowed to join a Class-3 virtual BSS; and

wherein a Class-3 virtual BSS is determined by the kind of authentication used to authenticate said station.

23. The network of Claim 22, wherein a Class-1 virtual BSSID is the BSSID field of every Class 1 and Class 2 frame that has such a field.

24. The network of Claim 22, wherein a Class-1 virtual BSSID is the receiver or transmitter address field, where appropriate, for Class 1 and Class 2 frames.

25. The network of Claim 7, wherein every virtual BSS has identical beacon frame content except for a Timestamp, Beacon interval, Capability information Privacy (Protected) bit, Service Set Identifier (SSID), security capability element, and Traffic Indication Map (TIM) element fields.

26. The network of Claim 22, wherein said PAP does not have to beacon for a Class-3 virtual BSS if it does not support Power-Save (PS) mode for end stations in that BSS;

wherein if said PAP does beacon for a Class-3 BSS, then an SSID element in every beacon specifies a broadcast SSID;

wherein a Class-3 virtual BSS is prevented from being identified through beaconing.

27. The network of Claim 26, wherein only a Class-1 virtual BSS beacon has an SSID element with a non-broadcast SSID field;

wherein a station can associate with a Class-1 virtual BSS only;

28. The network of Claim 22, wherein every station is by default a member of a Class-1 virtual BSS at a PAP;

wherein said PAP can either authenticate a user of said station or said station itself in said Class-1 virtual BSS;

wherein if successful, said station enters 802.11 State 2 at said PAP; and

wherein said PAP and said station can then exchange Class 1 and Class 2 frames while in said Class-1 virtual BSS.

29. The network of Claim 28, wherein Class 2 frames are protected cryptographically if said station and said PAP share a unicast security association after successful authentication.

30. The network of Claim 29, wherein said PAP and said station share a group security association after authentication;

wherein said group security association is for a Class-3 virtual BSS to which said station belongs if it completes an 802.11 Association with said PAP.

31. The network of Claim 30, wherein before said station and said PAP can exchange Class 3 frames, said station must request Association with said Class-1 virtual BSS from State 2; and switch to a Class-3 virtual BSS.

32. The network of Claim 31, wherein said PAP switches said station to a Class-3 virtual BSS by responding to said station's Association Request with an Association Response MMPDU whose source address (Address 2 Field) or BSSID (Address 3 field) is a Class-3 virtual BSSID for that virtual BSS.

33. The network of Claim 32, wherein said Class-3 virtual BSS is determined in one of the following ways:

an authentication server in said DS specifies a DSM VLAN for a user and said PAP maps it to a Class-3 virtual BSSID using its DSM VLAN mapping;

an authentication server in said DS specifies a Class-3 virtual BSS for said user; or

said PAP creates a new Class-3 virtual BSS for said user;

wherein said PAP may inform an authentication server of a new virtual BSS and provide it with rules for allowing other stations to join said new BSS.

34. The network of Claim 22, wherein a Class-1 virtual BSS is discovered through 802.11 beacon or Probe Response management frames, where a BSSID field (Address 3 field) and source address field (Address 2 field) are each set to a Class-1 virtual BSSID.

35. The network of Claim 22, wherein said PAP implements a MAC Protocol Data Unit (MPDU) bridge protocol which, for an MPDU received from either said DSM or said WM, said protocol addresses either of:

an MPDU received from said DSM, wherein:

a received MPDU has no VLAN tag or a null VLAN tag;

said MPDU from said DSM is relayed to a virtual BSS if said MPDU destination address is an address of a station that belongs to said virtual BSS and said station is associated with said PAP; or

if said MPDU destination address is a group address, said virtual BSS has a station that belongs to said group and said station is associated with said PAP; or

a received MPDU has a non-null VLAN tag;

said virtual BSS to which said MPDU is relayed is identified by said virtual BSSID to which said non-null VLAN tag is mapped under said PAP's DSM VLAN mapping; and

if said mapping is undefined for a given tag, said MPDU is not relayed;

wherein any virtual BSS to which a received MPDU is relayed has a BSSID which forms a source address (Address 2 field) of the 802.11 MPDU that is relayed to that virtual BSS; or

an MPDU received from said WM, wherein:

a received 802.11 MPDU is relayed to a virtual BSS identified by Address 1 field of said MPDU if said MPDU destination address (Address 3 field of MPDU) is an address of a station that belongs to said identified virtual BSS and said station is associated with said PAP; or

if said MPDU destination address is a group address;

otherwise, said frame is not relayed to any virtual BSS;

wherein Address 1 field of a received 802.11 MPDU is a source address (Address 2 field) of an 802.11 MPDU that is relayed to said virtual BSS identified by said Address 1 field.

36. The network of Claim 35, wherein said received MPDU is also relayed to said DSM if said destination address (Address 3 field of MPDU) is an address of a station that is not associated with said PAP; or

if said destination address is a group address;

wherein said MPDU relayed to said DSM has a VLAN tag if said DS is VLAN aware, and is untagged otherwise; and

wherein said VLAN tag is a pre-image of said Address 1 field of said received MPDU under said PAP's DSM VLAN mapping.

37. The network of Claim 22, further comprising:

means for performing encryption and decryption by applying 802.11 Data frames and Management frames of subtype Association Request/Response, Reassociation Request/Response, Disassociation and Deauthentication.

38. The network of Claim 37, wherein said encryption process used by said PAP before sending an 802.11 Data or Management frame to said WM comprises a mechanism that performs the steps of:

identifying a security association for said frame; and

then using said association to construct an expanded frame for transmission according to an encipherment and authentication code protocol.

39. The network of Claim 38, wherein if a frame destination address (Address 1 field) is the address of a station then a unicast security association shared between that station and said PAP is used in said frame expansion; and

wherein if said frame is a Data frame and its destination address is a group address then said MPDU bridge protocol identifies a destination virtual BSS for said frame, wherein a group security association for said identified virtual BSS is used in said frame expansion.

40. The network of Claim 39, wherein a non-PAP station transmits an 802.11 MPDU of type Data or Management to said DSM using a unicast security association it shares with said PAP in its virtual BSS.

41. The network of Claim 40, wherein when receiving an 802.11 Data or Management frame from said WM, said PAP attempts to decipher and verify integrity of said frame using a unicast security association for a station identified by a source address (Address 2 field) of said MPDU.

42. The network of Claim 41, wherein when receiving an 802.11 MPDU of type Data or Management from said PAP, a non-PAP station attempts to decipher and verify integrity of said frame using a unicast security association it shares with said PAP if a destination address of said frame (Address 1 field) is an address of said station, and by using a group security association of its Class-3 virtual BSS if said destination address of said frame is a group address.

43. A location-update method for updating forwarding tables of bridges, or other interconnection media, that connect Public Access Points (PAPs) together, where multiple PAPs are attached to different bridges in a spanning tree of a bridged LAN and an end station associates with one of said PAPs and then reassociates with a new PAP, comprising the steps of:

said new PAP sending a directed Bridge Protocol Data Unit (BPDU) to said PAP with which said station was previously associated;

wherein destination address of said BPDU is current access point (AP) address of a Reassociation Request frame, which is a Class-3 virtual BSS identifier (BSSID); and

wherein source address is a hardware address of said station;

upon receiving a relocation MPDU at a particular port, a bridge updating its forwarding table with an entry that binds a receiving port to a source address of said MPDU; and

said receiving bridge forwarding a relocation MPDU to its designated root port, unless said MPDU arrived on that port or said receiving bridge is a root of said spanning tree;

wherein if said MPDU is received at said designated root port of said bridge or by a root bridge then it is forwarded according to a learned forwarding table of said bridge, which optionally comprises flooding said MPDU to all ports except said receiving port.

44. A fine bridging method for a wireless network, comprising the steps of:

decoupling identification of a broadcast or multicast domain with a Basic Service Set (BSS); and

determining bridging behavior of an access point (AP) by a policy expressed as a directed graph;

wherein for a given policy, a broadcast domain for a node is itself and all nodes it must access;

wherein said broadcast domain set of said policy is a set of broadcast domains for its nodes; and

wherein nodes of said graph are stations and there is an edge from a first station to a second station if and only if said first station must be able to communicate with, or access said second station, such that said second station must be able to receive directed or group frames from said first station.

45. The method of Claim 43, further comprising the step of:

providing a group security association per broadcast domain.

46. The method of Claim 45, wherein each station (node) possesses a first group security association of a broadcast domain for itself in said policy, and a second set of group security associations, one for every other broadcast domain in said policy of which said station is a member.

47. The method of Claim 46, wherein said first group security association is used by said station for sending group frames and said second set of group security associations is used for receiving group frames.

48. The network of Claim 42, wherein broadcast and multicast traffic in different virtual basic service sets is protected with different encipherment or authentication-code protocols in said network.

49. The Network of Claim 42, where unicast traffic between a PAP and a station and between said PAP and another station in a virtual BSS is protected with different encipherment or authentication-code protocols in said virtual BSS.